<https://fontmeme.com/blade-runner-font/>  
(For name text)

Report by Chris H.   
Date of Completion:   
 *Note: This report details a penetration test conducted on a virtual system hosted on* [*https://www.hackthebox.eu/*](https://www.hackthebox.eu/) *. This system was a lab designed to practice penetration testing techniques, and is not a real-world system with PII, production data, etc.*

Target Information

|  |  |
| --- | --- |
| Name |  |
| IP Address |  |
| Operating System |  |

Tools Used

* Operating system: Kali Linux – A Linux distribution designed for penetration testing
* OpenVPN – An open-source program used for creating a VPN connection to hackthebox.eu servers, which allows for connection to the target.
* Nmap – A network scanner used to scan networks and systems. Discovers hosts, services, OS detection, etc.

Executive Summary

NAME OF BOX is a virtual system hosted on <https://www.hackthebox.eu/>. I conducted this penetration test with the goal of determining the attack surface, identifying the vulnerabilities and attack vectors, exploiting the vulnerabilities, and gaining root access to the system. All activities were conducted in a manner simulating a malicious threat actor attempting to gain access to the system.

The goal of the attack was to retrieve two files:

1) user.txt – A file on the desktop (Windows) or in the /home directory (Linux) of the unprivileged user. Contents of the file are a hash that is submitted for validation on hackthebox. Successful retrieval of this file is proof of partial access/control of the target.

2) root.txt – A file on the desktop (Windows) or in the /home directory (Linux) of the root/Administrator account. This file contains a different hash which is submitted for validation on hackthebox. Successful retrieval of this file is proof of full access/control of the target.

Summary of Results

Put summary here

Attack Narrative

Steps with screenshots go here

Vulnerability Detail and Mitigation

List the vulnerabilities and mitigations to secure the machine

Appendix 1: Full Nmap Results

Put nmap here